Blockchain consensus: From proof-of work to proof-of-stake

Jonathan Healy
jonathan.d.healy@gmail.com
January 2020

1. Introduction

With the introduction of Bitcoin in 2008 via the Bitcoin white paper [1], written by an author cloaked in anonymity – Satoshi Nakamoto - the notion of the blockchain was released on the world. The consensus model for this new concept was, and still is, generally called proof-of-work. Nodes in the network seeking to acquire rewards, associated with adding a block of transactions to the inter-connected chain of blocks that stretch right back to the very genesis block itself, compete to compute cryptographic puzzles. After a valid block of transactions is assembled and a hash containing enough leading zeroes is found for that block, the block is examined by other nodes in the network. If everything checks out, the block is added to the blockchain and other blocks will henceforth be added to it.

Process is important here of course because the system relies on it to provide security and ensure that the double-spending problem is solved. Solving this problem guarantees that the same unit of currency will not be spent twice. Prior to the introduction of Bitcoin this was something that was unsolved. Over the years confidence in Bitcoin has grown and today the network has a market cap of over $157 billion dollars, measured in US currency. There are two main criticisms of Bitcoin, however.

One criticism of Bitcoin is that the network is slow and the other concerns the vast amounts of energy via electricity that is presently being used to secure the Bitcoin blockchain. Both of these things can potentially be addressed by improving Bitcoin's consensus model. The most popular idea with respect to replacing proof-of-work is easily, proof-of-stake. In this system nodes are generally chosen to validate a block of transactions and receive the corresponding reward with the odds of doing so being based on the number of tokens that are held in a node's account [2,3,4].

2. Proof-of-Work (PoW)

Proof-of-work is a concept that has become famous via Bitcoin but it was not a new idea as of the publication of [1]. Hashcash [5] was originally proposed in 1997 as a means to, "throttle systematic abuse of un-metered internet resources such as email and anonymous remailers." Hashcash was described as a trapdoor-free cost function meaning that is was a cost function where a server would have no advantage in minting tokens. The idea is that by requiring proof-of-work, illegitimate entities would be unable to expend the effort needed to send out large amounts of spam. Interestingly one of the applications envisioned in [5] was as a minting mechanism for b-money which was proposed by Wei Dei [6] and is generally thought of as the precursor to Bitcoin.

3. Proof-of-Stake (PoS)

Unlike proof-of-work, proof-of-stake does not rely on solving difficult cryptographic puzzles in order for the network to reach consensus. There are many proposed ways to implement proof-of-stake but the general idea is that validators are chosen to lead any round with the odds stacked in their favor via the number of tokens that they hold. One popular offshoot is delegated proof-of-stake (DPoS). In DPoS there are only a certain number of validators in the network and token holders can vote for those validators by delegating their tokens to them.

One PoS proposal receiving a lot of attention is [4] as it being developed by the team behind Ethereum. Their PoS scheme – Casper - has been partially derived from Byzantine fault tolerance literature. Interestingly, it is designed as an overlay for PoW systems like Ethereum to offer PoS based security improvements. Implementing Casper on Ethereum would eventually lead to fully replacing PoW. Casper introduces the idea of slashing to combat undesirable behaviour in the network. PoS validators would have their stake locked away and their balances could be either diminished or even fully eliminated by the protocol.

4. Pure Proof-of-Stake (PPoS)

Algorand is a blockchain protocol headed by former Turing award winner Silvio Micali. Algorand uses an alternate version of proof-of-stake called pure proof-of-stake (PPoS). Although Algorand has evolved since the paper, ‘Algorand: Scaling Byzantine Agreements for Cryptocurrencies’ was published in 2017 the basics surrounding the protocol can be found in it [2].

Algorand implements a new Byzantine Agreement protocol to establish consensus. Verifiable Random Functions are used which allow network nodes to privately check if they have been selected to participate in assembling a new block. This same mechanism allows for nodes to include a proof of their selection in their network messages. Users therefore do not need to keep any private state except for their private keys which helps improve general security.

The protocol allows Algorand to replace participants immediately after they send a message. This helps PPoS to differentiate itself from most regular proof-of-stake schemes. In many implementations of PoS, prospective validators need to lock their funds into the system. Algorand allows Users to have free access to their funds while also enjoying the benefit of potentially receiving rewards for being chosen as a block validator. Having a larger pool of validators to choose from via the utilization of Verifiable Random Functions improves security because attacks carried out on a chosen group of validators is not as concerning anymore.

Results published [2] state that Algorand achieves a throughput over 125x greater than what can be achieved by Bitcoin with much faster block confirmation times to boot. Furthermore, the authors state that the network receives almost no penalty for scaling. The Algorand MainNet was launched in June 5 of 2019.

5. Federated Byzantine Agreement

Federated Byzantine Agreement (FBA) is a consensus model introduced to the world by Stanford professor David Mazieres in the paper, ‘The stellar consensus protocol: A federated model for internet level consensus’ published in 2015 [3]. Federated Byzantine Agreement differs from proof-of-stake because consensus is not carried out by nodes chosen with weight given to the number of tokens that they hold in the native currency.

In FBA, each participant or validator selects a subset of other nodes that it trusts and this group is sometimes called a, ‘quorum slice’. After considering a transaction, a participant waits for the vast majority of the nodes that it trusts to signal that they agree with the transaction. The nodes that the participants trust also have other nodes that they trust and they wait for those other nodes to decide before making their own decision on any transaction. In this way, the whole network soon agrees on a transaction and it becomes infeasible for an attacker to roll back a transaction. Stellar is a public blockchain network built on the FBA consensus model. To become a validator in the network and bootstrap into the system a participant just needs another validator to add them to their quorum slice.

References

1. Nakamoto, Satoshi. Bitcoin: A peer-to-peer electronic cash system. 2008.
2. Gilad, Yossi, et al. "Algorand: Scaling byzantine agreements for cryptocurrencies." Proceedings of the 26th Symposium on Operating Systems Principles. 2017.
3. Mazieres, David. "The stellar consensus protocol: A federated model for internet-level consensus." Stellar Development Foundation 32 (2015).

4. Buterin, Vitalik, and Virgil Griffith. "Casper the friendly finality gadget." *arXiv preprint arXiv:1710.09437* (2017).
5. Back, Adam. “Hashcash: A denial of service counter-measure (2002).
6. W. Dai, “b-money,” http://www.weidai.com/bmoney.txt, 1998.